5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,962	02/26/2002	Mark E. Larkin	4365/4	7747

7590 03/11/2004

Ralph F. Hoppin
Brown Raysman
900 Third Avenue
New York, NY 10022

EXAMINER	
PAPPAS, PETER	
ART UNIT	PAPER NUMBER
2671	

DATE MAILED: 03/11/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/083,962	LARKIN ET AL.	
	Examiner	Art Unit	
	Peter-Anthony Pappas	2671	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *28,29 and 31* is/are allowed.

6)☒ Claim(s) *1-12,21 and 30* is/are rejected.

7)☒ Claim(s) *13-20 and 22-27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: omitted application number (page 1, line 6).

Appropriate correction is required.

Allowable Subject Matter

2. Claims 28-29 and 31 are allowed.

3. In regards to claims 28 and 31 the prior art of record does not disclose or suggest a first grid of cells having each cell associated with a security event category and a temporal value, wherein said first grid of cells is connected to a second grid of cells via association lines.

4. Claims 13-20 and 22-27 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

5. In regards to claim 13 the prior art of record does not disclose or suggest a first graph having both a temporal axis and security category axis, wherein said first graph is connected to a second graph via association lines.

6. In regards to claim 22 the prior art of record does not disclose or suggest a first grid of cells having each cell associated with a security event category and a temporal value, wherein said first grid of cells is connected to a second grid of cells via association lines.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 10 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. In regards to claim 10 it is unclear as to whether all or only one of the listed event types must be selected. Therefore, the claim limitation is considered to read with later of the two possibilities.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-12, 21 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over the SilentRunner Discovery Visualization Analysis Training Manual (herein referred to as STM), in view of Maloney et al. (U.S. Patent No. 6, 304, 262 B1).

12. In regards to claim 1 the STM teaches that SilentRunner DVA system has the ability to produce a variety of 2D and 3D views to enhance the understanding of complex networks (section 3-1, section 3-2 and section 3-3, Fig. 3.2). The Collector LAN Engine (also referred to as CLE or Collector) monitors Ethernet LAN traffic and gathers data regarding a network, its structure, its method of operation, an its users. The CLE decodes the raw packet data and organizes it into a knowledgebase

(database) of information (section 3-3, ¶ 3-5). A packet log file maintained by the CLE (considered part of said knowledgebase) contains information about each packet captured, including date and time, source and destination IP address (network element), source and destination MAC address, protocol used (security event), and port numbers (section 4-3, ¶ 4).

The Link Notebook application allows for the creation of "link charts" or diagrams from data collected by the CLE (section 8-3, ¶ 1). The figure entitled "Link Study by Protocol Count" visually depicts categories of select protocols (security events) in a first section of display space (elements B) as well as visually depicts IP addresses (network elements) in a second section of said display space (elements A). Association lines (elements C), indicated by lines where one end terminates in an arrow, are displayed between groupings of a select numbers of protocols and IP addresses (section 8-24 and section 8-12, Fig. 8.9).

STM fails to explicitly teach simulating 3D space on a 2D display device. Maloney et al. teaches a software system which enables computer code analysis and the 3D visualization and animation of network traffic and structure (see column 2, lines 1-11). The 3D display 24 adds a third dimension to any of the data collect by the discovery tool 12 to view, animate, and analyze complex nodal diagrams in 3D space.

It would have been obvious to one skilled in the art, at the time of the applicant's invention, to add a third dimension to the display of data, presented in two dimensions, because the addition of a third vector would permit for the simultaneous viewing of large complex diagrams on interconnected planes as well as allow for the rotation of the

diagrams on any axis thereby viewing relationships that would otherwise become obscured when viewed on 2D planes (column 11, lines 26-38, and Fig. 1).

13. In regards to claim 2 the rationale disclosed in claim 1 is incorporated herein. STM teaches the various components for the diagramming tool (section 8-3, ¶ 6). Elements A (sections 8-12 and 8-24) are considered to represent host computer systems. It is noted that a network element (i.e. IP address) is used to identify a system to which it corresponds, such as host computer system, and therefor is considered one in the same.

14. In regards to claim 3 the rationale disclosed in claim 1 is incorporated herein. Said categories are represented by elements B (first graphical objects) and said network elements are represented by elements A (second graphical objects).

15. In regards to claim 4 said second graphical object is considered an image of a host computer system (section 8-12, Fig. 8.9, and section 8-24).

16. In regards to claim 5 STM teaches varying screen positions of geometrical objects, representative of network elements (section 8-12, Fig. 8.9, and section 8-24).

17. In regards to claim 6 STM teaches the use of text (i.e. an alpha-numeric IP address) describing a geometric object (section 8-12, Fig. 8.9, and section 8-24).

18. In regards to claim 7 said "link chat" or diagram is considered a graph. STM teaches varying screen positions of first graphical object (section 8-12, Fig. 8.9, and section 8-24).

19. In regards to claim 8 STM teaches the use of text with elements B (section 8-12, Fig. 8.9, and section 8-24).

20. In regards to claim 9 STM teaches a plurality of visual depictions of associations (trusted relationships) between host computer systems which are achieved through the use of said association lines. It is noted that the connection of a plurality of host computer systems, utilizing any number of protocols, is considered to involve the mutual accessing of data by said plurality of host computer systems.

21. In regards to claim 10 it is noted that network protocols (i.e. HTTP, HTTPS, POP3, etc.) are considered forms of network access.

22. In regards to claim 11 STM teaches that a packet log file (considered part of said knowledgebase) maintained by the CLE contains information about each packet captured, including date and time, source and destination IP address, source and destination MAC address, protocol used, and port numbers (section 4-3, ¶ 4). It is noted that said stored IP address (source/destination) information and port number information are considered first and second properties, respectively, of a given network element.

23. In regards to claim 12 the rationale disclosed in the rejection of claim 4 is incorporated herein.

24. In regards to claim 21 the rationale disclosed in the rejection of claim 1 is incorporated herein.

25. In regards to claim 30 the rationale disclosed in the rejection of claim 1 is incorporated herein. It is noted that said SilentRunner DVA system is considered to be implement via computer software (section 3-1 and section 3-2).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Schwuttke et al. (U.S. Patent Number 6, 222, 547 B1). Schwuttke et al. teaches that both static and dynamic information, gathered from monitored systems, is displayed in 3D cybersapce representations definining a virtual universe having three dimensions.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter-Anthony Pappas whose telephone number is 703-305-8984. The examiner can normally be reached on M-F 9:30am-7pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mark Zimmerman can be reached on 703-305-9798. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Peter-Anthony Pappas
Examiner
Art Unit 2671

PAP

MARK ZIMMERMAN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600